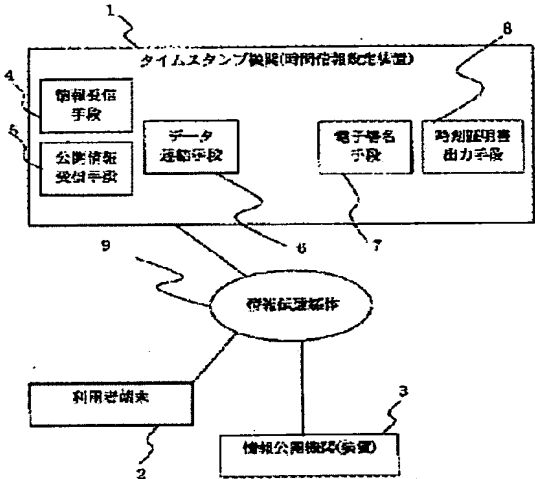


**TIME INFORMATION SETTING DEVICE AND TIME CERTIFICATION
VERIFICATION DEVICE**

Patent number: JP2002215825
 Publication date: 2002-08-02
 Inventor: MIYAZAKI KAZUYA; KAMOSHITA AKITERU; TOGASHI MASATAKA
 Applicant: MITSUBISHI ELECTRIC CORP
 Classification:
 - international: G09C1/00; G09C1/00; (IPC1-7): G06F17/60; G09C1/00
 - european:
 Application number: JP20010007507 20010116
 Priority number(s): JP20010007507 20010116

Report a data error here

Abstract of JP2002215825
PROBLEM TO BE SOLVED: To provide a technology to make impossible to set up the certification time before the time to be certified in connection with a time information setting device setting up certification time to material objects and information and the time certification verification device verifying the certification time. **SOLUTION:** A data connecting means 6 connects information received by an information receiving means 1 and open information (information not predictable beforehand; e.g. news, stock price or the like) received by an open information receiving means 5, creates a time certificate by adding an electronic signature by an electronic signature means 7 and outputs the created time certificate by a time certificate output means 8.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-215825
(P2002-215825A)

(43) 公開日 平成14年8月2日(2002.8.2)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 17/60	1 4 0 Z E C 3 0 2 5 1 2 6 4 0	G 0 6 F 17/60	1 4 0 Z E C 3 0 2 E 5 1 2 6 4 0 Z
G 0 9 C 1/00		G 0 9 C 1/00	

審査請求 未請求 請求項の数9 O L (全 9 頁)

(21) 出願番号 特願2001-7507(P2001-7507)

(22) 出願日 平成13年1月16日(2001.1.16)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 宮崎 一哉

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 鴨志田 昭輝

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100099461

弁理士 溝井 章司 (外2名)

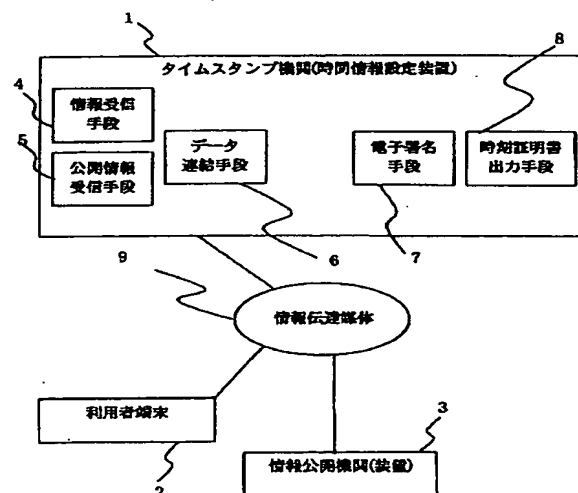
最終頁に続く

(54) 【発明の名称】 時間情報設定装置及び時刻証明検証装置

(57) 【要約】

【課題】 有体物や情報に対して証明時刻を設定する時間情報設定装置および、その証明時刻を検証する時刻証明検証装置に係り、証明時刻以前にその証明時刻を設定できないようにする技術を提供することを課題とする。

【解決手段】 データ連結手段6は、情報受信手段1で受信した情報と、公開情報情報受信手段5で受信した公開情報（例えば、ニュースや株価情報などの事前に予測できない情報）とを連結し、更に、電子署名手段7により、電子署名を付加することにより時刻証明書を生成し、生成した時刻証明書を時刻証明書出力手段8より出力する。



【特許請求の範囲】

【請求項1】 事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする時間情報設定装置（1）時刻証明の対象となる対象情報を受信する情報受信手段、（2）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（3）受信した上記対象情報と、受信した上記公開情報とを連結し、連結したデータを生成するデータ連結手段、

（4）上記連結したデータに電子署名を付加する電子署名手段、（5）上記連結したデータと、付加された上記電子署名とを含む時刻証明情報を出力する時刻証明書出力手段。

【請求項2】 上記データ連結手段は、上記対象情報と、上記公開情報とに加えて、更に、証明する日時を示す日時情報を連結することを特徴とする請求項1記載の時間情報設定装置。

【請求項3】 事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする時間情報設定装置（1）時刻証明の対象となる対象情報を受信する情報受信手段、（2）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（3）受信した上記対象情報を縮約し、縮約した上記対象情報と、受信した上記公開情報と、証明する日時を示す日時情報とを連結し、連結したデータを生成するデータ連結手段、（4）上記連結したデータに電子署名を付加する電子署名手段、（5）上記連結したデータと、付加された上記電子署名とを含む時刻証明情報を出力する時刻証明書出力手段、（6）上記連結したデータを公開する情報公開手段。

【請求項4】 上記情報公開手段は、上記連結したデータを縮約し、縮約したデータを公開することを特徴とする請求項3記載の時間情報設定装置。

【請求項5】 事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする時間情報設定装置（1）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（2）受信した上記公開情報と、証明する日時を示す日時情報とを連結し、連結したデータを生成するデータ連結手段、（3）上記連結したデータに電子署名を付加する電子署名手段、（4）上記連結したデータと、付加された上記電子署名とを表わす印刷形態を生成する時刻証明フォーマット生成手段、（5）生成した印刷形態を印刷する印刷手段。

【請求項6】 上記印刷手段は、貼り換えできないシールに印刷することを特徴とする請求項5記載の時間情報設定装置。

【請求項7】 上記印刷手段は、時刻証明の対象となる

物品に直接印刷することを特徴とする請求項5記載の時間情報設定装置。

【請求項8】 以下の要素を有することを特徴とする時刻証明検証装置（1）事前に予期できない事象についての公開情報と、証明する日時を示す日時情報と連結した連結データと、上記連結データに付加された電子署名とを表わす印刷形態を読み取る読み取り手段、（2）読み取った印刷形態に表わされている上記連結データと上記電子署名の検証を行う検証手段、（3）検証結果を出力する出力手段。

【請求項9】 上記出力手段は、上記検証結果と併せて、検証の対象となる商品の価格情報と、商品の名称とを印刷することを特徴とする請求項8記載の時刻証明検証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、有体物や情報に対する時刻の設定および検証方法に関するものである。より詳しくは、ソフトウェア、データ、情報、あるいは製品に対して、生成、保存等の事象が発生した時刻あるいは存在している時刻を保証するための時刻の設定および検証方法に関するものである。

【0002】

【従来の技術】図12は、例えば、特表平6-501571に示された従来のタイムスタンプ方式のフローチャートを示している。図12に基づいて従来の時間情報設定及び検証方式の動作を説明する。まず、著者が時刻情報の設定対象である数値文書（デジタルデータのこと）を用意する（ステップS1001）。次にその文書のハッシュを生成し（ステップS1002）、そのハッシュを時刻情報を設定するタイムスタンプ機関に送信する（ステップS1003）。すると、タイムスタンプ機関はそのハッシュと時刻データを連結した受理書を作成し（ステップS1004）、その受理書と現在の連鎖値を連結する（ステップS1005）。次に、タイムスタンプ機関は受理書と現在の連鎖値を連結したデータのハッシュを生成して新しい連鎖値とし（ステップS1006）、その新しい連鎖値を記した証明書を著者に送る（ステップS1007）。

【0003】従来の時間情報設定および検証方式は、上記のように連鎖値を利用して時刻情報を設定するものであったため、文書を登録した順序の改ざんが困難となり、文書登録順序は保証されることになる。しかし、証明書に表される時刻そのものの正当性を保証するものではない。つまり、時系列順にならべられた文書に対する時刻が揃って大きく前後にずれている可能性を否認しないという問題点があった。

【0004】また、時刻を表すデータは一般に時刻を示す数値あるいは文字列で与えられるため、利用者に対して直感的にそれが正確な時刻であることを認識させられ

るものではない。つまり、基となる時計が狂っているかもしれない、あるいは時刻を示す数値や文字列に誤植があるかもしれないと思わせる可能性があるという問題点があった。

【0005】

【発明が解決しようとする課題】この発明は上記のような問題点を解決するためになされたもので、時刻の保証、特に時刻情報を生成する際に、時刻情報を生成する正にその時刻において、その時刻以降の時刻を表す時刻情報を生成できないことを保証することを目的とする。また、時刻情報が表している時刻が、利用者に対して直感的にその当時の正しい時刻であることを認識させ易いものとするを目的とする。これにより、時刻の不正表示を防止し、時刻データとしての正確性の確保が可能となり、例えば、生鮮食料品の製造、発送、鶏卵の産出時刻、発送、調理品の製造、あるいは情報の生成あるいは登録等に対し時刻を偽ることを防止する。

【0006】

【課題を解決するための手段】この発明に係る時間情報設定装置は、事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする。

(1) 時刻証明の対象となる対象情報を受信する情報受信手段、(2) 情報公開機関装置から、上記公開情報を受信する公開情報受信手段、(3) 受信した上記対象情報と、受信した上記公開情報とを連結し、連結したデータを生成するデータ連結手段、(4) 上記連結したデータに電子署名を付加する電子署名手段、(5) 上記連結したデータと、付加された上記電子署名とを含む時刻証明情報を出力する時刻証明書出力手段。

【0007】上記データ連結手段は、上記対象情報と、上記公開情報とに加えて、更に、証明する日時を示す日時情報を連結することを特徴とする。

【0008】この発明に係る時間情報設定装置は、事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする。(1) 時刻証明の対象となる対象情報を受信する情報受信手段、(2) 情報公開機関装置から、上記公開情報を受信する公開情報受信手段、(3) 受信した上記対象情報を縮約し、縮約した上記対象情報と、受信した上記公開情報と、証明する日時を示す日時情報とを連結し、連結したデータを生成するデータ連結手段、(4) 上記連結したデータに電子署名を付加する電子署名手段、(5) 上記連結したデータと、付加された上記電子署名とを含む時刻証明情報を出力する時刻証明書出力手段、(6) 上記連結したデータを公開する情報公開手段。

【0009】上記情報公開手段は、上記連結したデータを縮約し、縮約したデータを公開することを特徴とする。

【0010】この発明に係る時間情報設定装置は、事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする。(1) 情報公開機関装置から、上記公開情報を受信する公開情報受信手段、(2) 受信した上記公開情報と、証明する日時を示す日時情報とを連結し、連結したデータを生成するデータ連結手段、(3) 上記連結したデータに電子署名を付加する電子署名手段、(4) 上記連結したデータと、付加された上記電子署名とを表わす印刷形態を生成する時刻証明フォーマット生成手段、(5) 生成した印刷形態を印刷する印刷手段。

【0011】上記印刷手段は、貼り換えできないシールに印刷することを特徴とする。

【0012】上記印刷手段は、時刻証明の対象となる物品に直接印刷することを特徴とする。

【0013】この発明に係る時刻証明検証装置は、以下の要素を有することを特徴とする。(1) 事前に予期できない事象についての公開情報と、証明する日時を示す日時情報と連結した連結データと、上記連結データに付加された電子署名とを表わす印刷形態を読み取る読み取り手段、(2) 読み取った印刷形態に表わされている上記連結データと上記電子署名の検証を行う検証手段、(3) 検証結果を出力する出力手段。

【0014】上記出力手段は、上記検証結果と併せて、検証の対象となる商品の価格情報と、商品の名称とを印刷することを特徴とする。

【0015】

【発明の実施の形態】実施の形態1。図1は、実施の形態1におけるブロック図である。図1において、1は、利用者からの時刻証明情報の設定要求に応じて要求された情報に対して時刻証明情報を生成し、発行するタイムスタンプ機関(時間情報設定装置)、2は、タイムスタンプ機関1に対してある情報に対する時刻証明情報を要求する利用者端末、3は、タイムスタンプ機関1が時刻証明情報を作成するときに利用する公開情報を発行する情報公開機関(装置)、4は、利用者端末2から送られてくる情報であって、時刻保証情報を発行する対象となる情報(対象情報)を受信する情報受信手段、5は、情報公開機関3が発行した公開情報を受信する公開情報受信手段、6は、情報受信手段4が受信した情報と公開情報受信手段5が受信した公開情報を連結するデータ連結手段、7は、データ連結手段6が連結したデータに電子署名を付加する電子署名手段、8は、電子署名手段7により得られた電子署名と縮約されたデータを含む時刻証明書を利用者端末2に向けて出力する時刻証明書出力手段、9は、タイムスタンプ機関1と利用者端末2と情報公開機関(装置)3の間で情報を交換するための情報伝達媒体(例えば、インターネットのようなネットワークを含む)である。

【0016】次に動作について説明する。まず、ある情報に対する時刻証明を得たい利用者が、利用者端末2から情報伝達媒体10を通して、タイムスタンプ機関1に対して情報あるいはそのメッセージ縮約を伴ったタイムスタンプ要求を送付する。

【0017】タイムスタンプ要求を受け取ったタイムスタンプ機関1は、情報公開機関3より受け取った公開情報を利用して時刻証明書を作成し、それを利用者端末2に送信する。

【0018】上記動作のうち、特に、タイムスタンプ機関1における動作の詳細をフローチャートに基づいて説明する。図2は、実施の形態1におけるタイムスタンプ機関の動作を示すフローチャートである。まず、情報受信手段4により、利用者から時刻証明の対象となる情報dを取得する(ステップ101)。時刻証明の対象となる情報は、文書、動画、静止画、音声などを表すバイナリデータである。

【0019】その直後あるいは同時に公開情報受信手段5により情報公開機関3が発行した公開情報pを取得する(ステップ102)。公開情報は、文書、動画、静止画、音声などを表すバイナリデータであり、時々刻々と変化する自然現象や社会現象に伴うものであり、事前に予期できない情報である。例えば、通信社によるニュース速報、株価情報、為替レート、TV放送、ラジオ放送、気象情報、気象衛星による雲の画像などを表すデータであり、そのデータを示すと日時が特定できることが条件となる。即ち、公開情報pの表す事象の日時tが周知であったり、情報公開機関3に日時tを照会できるなど、公開情報pから日時tが直ちに得られるものとする。このような公開情報のうち、最新のものを受信し、使用する。

【0020】次にステップ1とステップ2で得たデータをデータ連結手段6により連結し(ステップ103)、電子署名手段7によりそのデータ(d+p)に対するタイムスタンプ機関1の電子署名 $S_t(d+p)$ を生成する(ステップ104)。電子署名の方法は、MD2やMD5等のアルゴリズムによりデータのハッシュ値を取り、その値をRSA公開鍵暗号系の秘密鍵で暗号化するなどによる。

【0021】そして、連結したデータ(d+p)と電子署名 $S_t(d+p)$ を含む、情報dに対する時刻tの時刻証明書 $C_t(d)$ を生成/出力する(ステップ105)。図3は、実施の形態3における時刻証明書 $C_t(d)$ の構成を示す図である。

【0022】なお、時刻証明書 $C_t(d)$ には連結したデータ(d+p)そのものではなく、利用者が利用できるそれぞれのデータに対するポインタや識別子でもよい。つまり、ポインタの先の情報が厳重に管理され、後から改ざんできないように管理されている場合には、データの構成のうち(d+p)を(dへのポインタ+pへ

のポインタ)に置き換えることにより、リソースの節約を図ることができる。

【0023】以上のように、時刻証明書にタイムスタンプ機関1の電子署名 $S_t(d+p)$ を含むため、タイムスタンプ機関1が情報dと公開情報pの関係を保証することとなる。公開情報pは、その事象が生じた日時がtであることが周知であるか、あるいは第三者である情報公開機関3が公開情報pの発生日時tを保証するものであるため、単に数値データとして日時を添付するよりも直感的に日時を把握し易い。また、事前に予期できない情報を利用しているため、タイムスタンプ機関1が時刻証明書作成時tに偽ってt以降の時刻t'を付与することはできない。つまり、時刻証明書が作成された日時が時刻証明書の示す日時以前でないことを確実に保証することができる。

【0024】実施の形態2、以上の実施の形態では、時刻証明書を作成する際に時刻証明の対象となる情報と公開情報を利用したが、本実施の形態では、更に時刻情報を時刻証明書に含める。図4は、実施の形態2におけるブロック図である。図において、1~9は図1のものと同様であり、10は、時刻情報を示すデータを生成する時刻データ生成手段である。

【0025】次に動作について説明する。基本的な動作は実施の形態1と同様である。異なるのは、図2におけるステップ2とステップ3において、時刻データ生成手段10により日時を示すデータtを生成し、データ連結手段6によって時刻データtを時刻証明の対象となる情報dと公開情報pと連結し、時刻tの情報を含む時刻証明書を生成するところである。これにより、情報dの時刻tに対する時刻証明書 $C_t(d)$ には、タイムスタンプ機関1の電子署名 $S_t(t+d+p)$ が含まれることになる。図5は、実施の形態2における時刻証明書 $C_t(d)$ の構成を示す図である。

【0026】以上のように、時刻データtを含めることにより、時刻証明書から日時を直接認識することが可能である。また、必要に応じて、公開情報の示す日時と照合することにより、時刻データが示す日時の正否を確認できる。

【0027】実施の形態3、以上の実施の形態では、タイムスタンプ機関は特に外部に情報も公開しないものであるが、本実施の形態では、タイムスタンプ機関が外部に対して情報公開する。

【0028】図6は、実施の形態3におけるブロック図である。図6において、1~10は図4のものと同様であり、11は、時刻証明情報やその部分的な情報を公開する情報公開手段である。

【0029】次に動作について説明する。図7は、実施の形態3における動作を示すフローチャートである。基本的な動作は、実施の形態2のものの一部を除いて同様であり、異なるのは図2におけるステップ103以降に

相当する部分のみである。まずステップ111で、利用者より利用者情報受信手段4により情報dを受ける。次にステップ112で、公開情報受信手段5により公開情報pを受ける。次にステップ113で、時刻情報生成手段10により時刻を表すデータtを生成する。次にステップ114で、データ連結手段6により、情報dのハッシュ値H(d)を計算し、時刻t、公開情報pと連結する。次にステップ115で、電子署名手段7により、電子署名S t (t+H(d)+p)を生成する。次にステップ116で時刻証明書出力手段8により電子署名S t (t+H(d)+p)と連結したデータ(t+H(d)+p)を含む情報dに対する時刻証明書C t (d)を生成/出力する。図8は、実施の形態3における時刻証明書C t (d)の構成を示す図である。

【0030】次に、情報公開手段11により、連結したデータ(t+H(d)+p)あるいはそのハッシュ値H(t+H(d)+p)を含む情報を公開する。これらの情報を公開する手段は、例えば、CD-ROMに格納して配布する、定期刊行物に印刷して発行する、大手の新聞に掲載する、顧客や顧問弁護士に電子メールで送付するなどがある。

【0031】以上のように、(t+H(d)+p)を公開するようにしているので、情報dが時刻tに存在していたことを証明するために、周知にされた情報(t+H(d)+p)を利用することによって説明することができる。情報dの秘匿性を保ちつつ、少なくとも情報dは(t+H(d)+p)が公開された時刻t1よりも以前に存在していたことが保証される。

【0032】また、この公開情報を利用して自己あるいは他のタイムスタンプ機関が時刻証明書を生成できる。この場合、利用された公開情報に含まれる情報dがその公開情報を利用して生成された時刻証明書に含まれる情報d1よりも早い時期に位置するものとして説明でき、更に同様の情報公開およびその公開情報の利用を繰り返すことにより、情報間の前後関係を改ざんすることが困難になり、情報d、d1、d2・・・が時系列上に配置されることを保証できるようになる。

【0033】実施の形態4. 以上の実施の形態では、時刻証明の対象を無体物である情報としたものであるが、本実施の形態では、有体物に時刻証明をつける形態を説明する。図9は、実施の形態4におけるブロック図である。図9において、1、3、5～7、9、10は図1のものと同様であり、12は、公開情報と時刻情報を連結したデータとそれに対する署名をから、それらを含む情報を表す印刷形態(例えば、数値列、バーコード、あるいは図形など)を生成する時刻証明フォーマット生成手段、13は、対象となる有体物に対して時刻証明フォーマット生成手段12が生成した印刷形態を印刷する印刷手段である。

【0034】次に動作について説明する。時間と共に変

化する公開情報pと時刻データtから電子署名手段7で電子署名S t (t+p)を生成するところまでは、連結や電子署名の対象に利用者端末2からの情報dを含めない点を除き、同様である。

【0035】次に、時刻証明フォーマット生成手段12が、公開情報p、時刻データt、電子署名S t (t+p)から、人間あるいは機械が読み取れる形式(数字列、バーコード、図式表現など)を作成する。

【0036】そして最後に、印刷手段13により、時刻証明を付したい対象の有体物に印刷する。この時、容易に消去したり改ざんできない方法により印刷することが望ましい。また、時刻証明を有体物に直接印刷するのではなく、貼り換えの不可能あるいは張り替えたことが容易に検知できるようなシールに印刷し、それを対象の有体物に貼り付けるようにしてもよい。

【0037】以上のように、時間と共に変化する公開情報を含む時刻証明情報を対象物に印刷するようにしているので、時刻証明を与える者が予め未来の時刻を対象物に与えることができない。例えば、生鮮食料品に製造年月日や加工日時などを偽って未来の時刻を付しておき、顧客に対して新鮮であると誤解させることができなくなる。また、機械が読み取れる形式であるため、時刻証明を読み取り、署名の検証による改ざんチェックを行い、検証結果を表示するような装置が容易に実現できる。

【0038】実施の形態5. 実施の形態4は、時刻証明を生成し、それを有体物に添付する手段を示したものであるが、本実施の形態では、有体物に添付された時刻証明を検証する装置を示す。

【0039】図10は、時刻証明検証装置を示すブロック図である。14は、時刻証明検証装置、15は、機械が読み取れる形式(数字列、バーコード、その他の図式表現など)で印刷された時刻証明データを読み取る読み取り手段、16は、読み取った時刻証明を検証する検証手段、17は、検証結果を表示あるいは印刷する表示・印刷手段である。

【0040】次に動作について説明する。まず、有体物に添付された機械が読み取れる形式(数字列、バーコード、その他の図式表現など)で印刷された時刻証明データを読み取り手段15が読み取る。読み取ったデータには、公開情報p、時刻データt、電子署名S t (t+p)が含まれる。次に、検証手段16が、時刻データtと公開情報pを連結したデータ(t+p)と電子署名S t (t+p)により、電子署名検証を行なう。電子署名検証に用いる公開鍵は、検証を行なう機関が別途データベースに保管しておくか、あるいは第三者機関が認証書として発行しているものを用いる。

【0041】また、検証手段16は、電子署名検証の前あるいは後に、公開情報pの発生時刻を取得し、時刻データtとの比較を行なう。公開情報pの発生時刻は、公開情報pを公開する機関に対してオンラインで照会する

ことにより、得られるものとする。照会の際には公開情報pを送付する。また、時刻データtと公開情報pから得られた発生時刻に予め設定したしきい値以上の差がある場合には、時刻証明自体を信用しないこととし、検証を失敗することにする。

【0042】次に、表示・印刷手段17によって、検証が成功した場合は、時刻データtをディスプレイに表示あるいは紙に印刷する。なお、本装置は商品の小売店が商品の販売時に利用するPOS端末に組込まれていてもよく、この時、読み取り手段15は、時刻証明データと共に商品データを読み取り、検証結果を表示あるいは印刷する際に、小売店が管理するデータベースから引き出した該当する商品の名称と価格データと共に時刻データを表示し、レシートに印刷するようにしてもよい。

【0043】以上のように、有体物に添付された時刻証明データを読み取り、検証し、表示・印刷するようにしているので、その有体物に時刻証明データが添付された時期が、付随する公開情報の発生時刻よりも後であることを保証し、それを利用者に示すことができる。図11に、時間経過の概念を示す。また、時刻証明データには、時刻証明データの添付者の電子署名が付随するため、他の者が偽って異なった時刻証明データを添付することができない。従って、例えば、生鮮食料品の製造、発送、鶏卵の産出時刻、発送、調理品の製造等に対し、予め将来の時刻を偽って添付すること、あるいは小売店で新たな時刻証明を偽って添付することを防止できる。

【0044】最後に、時刻証明書を用いる検証について補足する。検証としては、以下のように署名の検証、時刻の検証、情報の検証が行われる。

・署名の検証

時刻証明情報Ct(d)の電子署名Stを検証する(実施の形態1, 2, 3)。

・時刻の検証

時刻証明情報Ct(d)の時刻tを得る(実施の形態2, 3のみ)。時刻証明情報Ct(d)内の公開情報pの発生時刻を公開情報の情報源により確認する(実施の形態1, 2, 3)。

・情報の検証

時刻証明情報Ct(d)の情報dを得る(実施の形態1, 3のみ)。時刻証明情報Ct(d)内の情報のハッシュ値H(d)と情報dを照合する(実施の形態2のみ)。以上の検証を実施することにより、確認した時刻tには情報dが既に存在していたことを確認することができる。

【0045】なお、上述の時刻は、原則として日付を含む概念であるが、証明のサイクルが短い場合には、日付を含まなくても有効なことがある。

【0046】上述の時間情報設定装置及び時刻証明検証装置は、コンピュータであり、各要素は、プログラムにより処理を実行することができる。また、プログラムを記憶媒体に記憶させ、記憶媒体からコンピュータに読み取られるようにすることができる。

【0047】

【発明の効果】本発明により、時刻情報を生成する際に、時刻情報を生成する時刻において、その時刻以降の時刻を表す時刻情報を生成できないことを保証することができる。また、時刻情報が表している時刻が、利用者に対して直感的にその当時の正しい時刻であることを認識させやすいものとすることができる。

【図面の簡単な説明】

【図1】 実施の形態1におけるブロック図である。

【図2】 実施の形態1におけるタイムスタンプ機関の動作を示すフローチャートである。

【図3】 実施の形態1における時刻証明書Ct(d)の構成を示す図である。

【図4】 実施の形態2におけるブロック図である。

【図5】 実施の形態2における時刻証明書Ct(d)の構成を示す図である。

【図6】 実施の形態3におけるブロック図である。

【図7】 実施の形態3における動作を示すフローチャートである。

【図8】 実施の形態3における時刻証明書Ct(d)の構成を示す図である。

【図9】 実施の形態4におけるブロック図である。

【図10】 時刻証明検証装置を示すブロック図である。

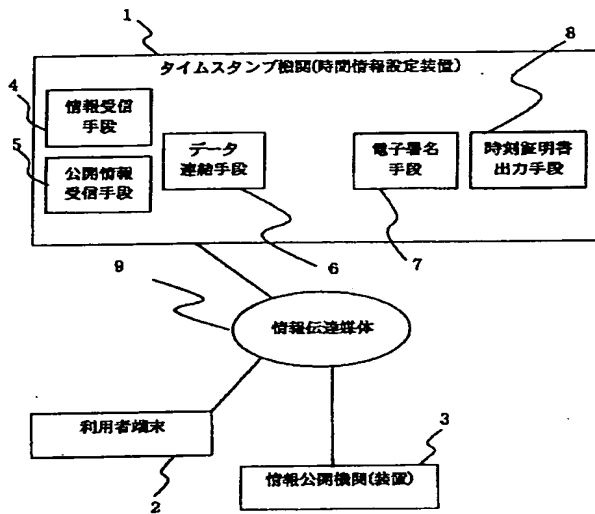
【図11】 時間経過の概念を示す。

【図12】 特表平6-501571に示された従来のタイムスタンプ方式のフローチャートを示している。

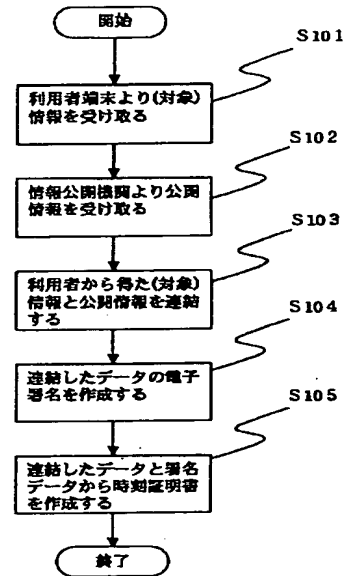
【符号の説明】

1 タイムスタンプ機関、2 利用者端末、3 情報公開機関、4 情報受信手段、5 公開情報受信手段、6 データ連結手段、7 電子署名手段、8 時刻証明出力手段、9 情報伝達媒体、10 時刻データ生成手段、11 情報公開手段、12 時刻証明フォーマット生成手段、13 印刷手段、14 時刻証明検証装置、15 読み取り手段、16 検証手段、17 表示・印刷手段。

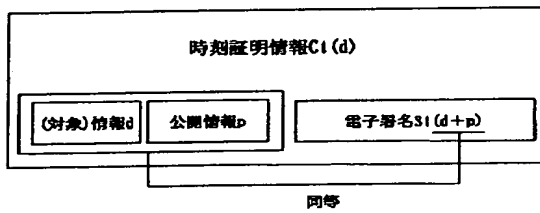
【図1】



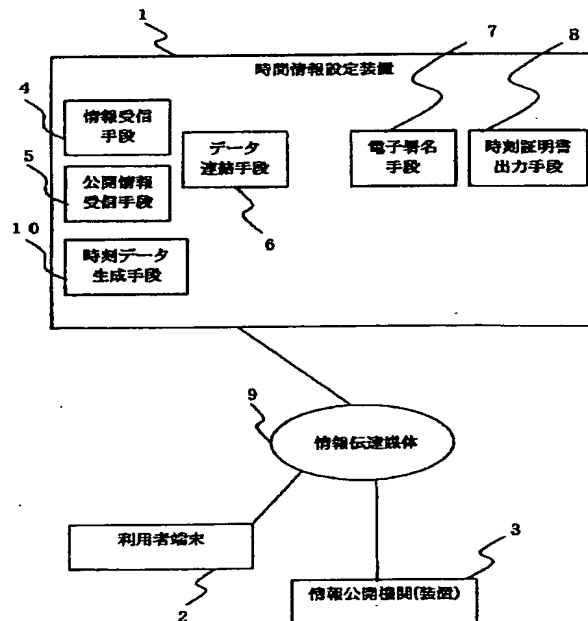
【図2】



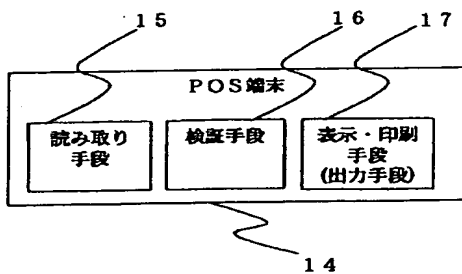
【図3】



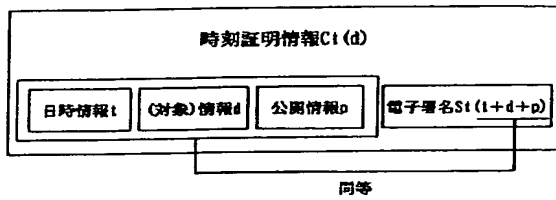
【図4】



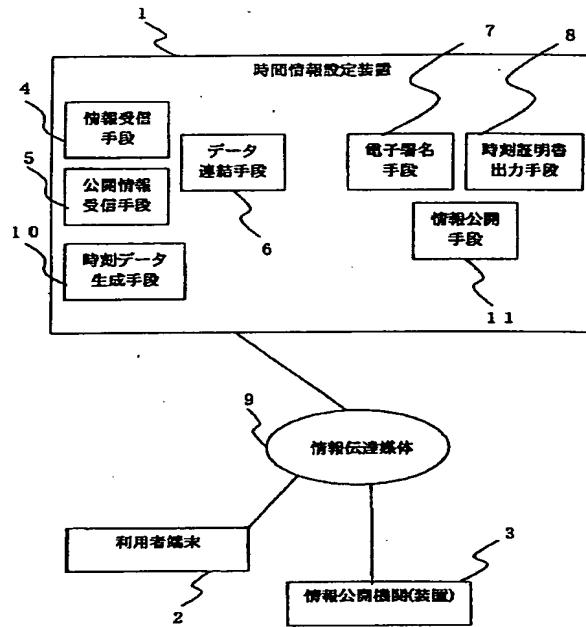
【図10】



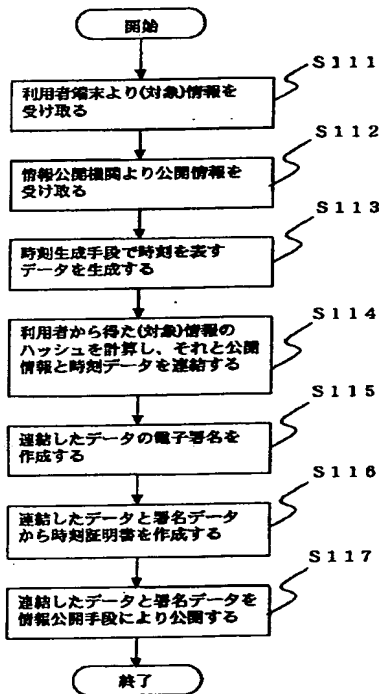
【図5】



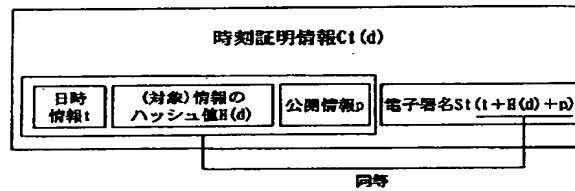
【図6】



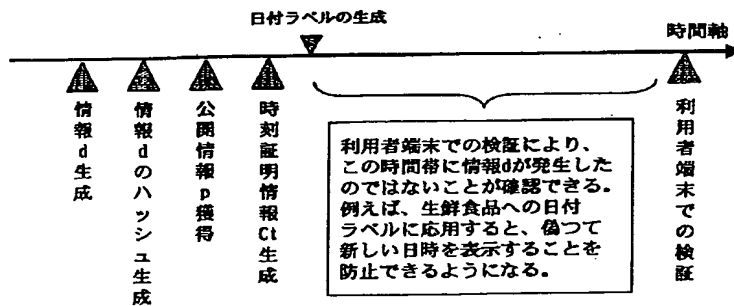
【図7】



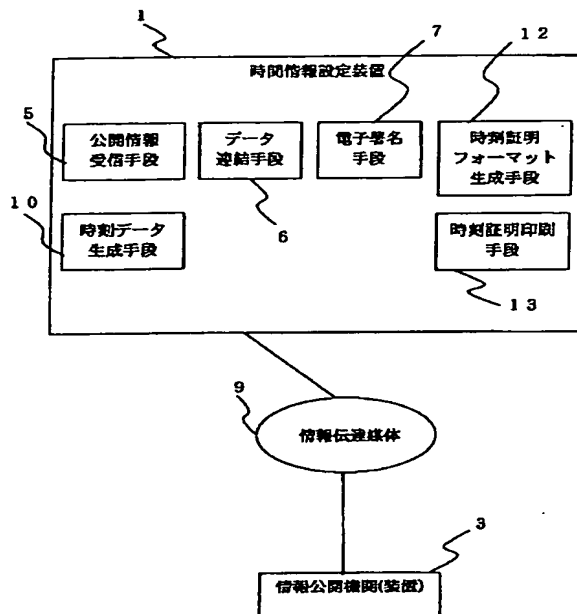
【図8】



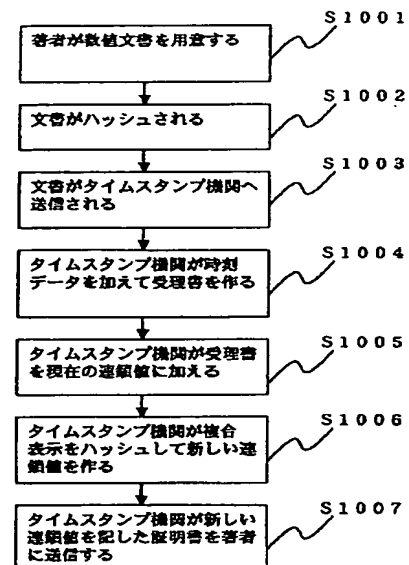
【図11】



【図9】



【図12】



フロントページの続き

(72)発明者 富樫 昌孝
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

Fターム(参考) 5J104 AA09 AA11 LA06